



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/777,661	02/13/2004	Serge Vaudenay	3829-021-27	5640
24510	7590	12/10/2007		
DLA PIPER US LLP ATTN: PATENT GROUP 500 8th Street, NW WASHINGTON, DC 20004-2131			EXAMINER SIMITOSKI, MICHAEL J	
			ART UNIT 2134	PAPER NUMBER
			MAIL DATE 12/10/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/777,661

Applicant(s)

VAUDENAY ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 2 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 13 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☒ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1-13 is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☒ Claim(s) 2-7, 9 and 11-13 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119


- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
- Paper No(s)/Mail Date 3/22/2005.

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

  
KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER

#### **DETAILED ACTION**

1. The IDS of 3/22/2005 was received and considered.
2. Claims 1-13 are pending.

#### ***Specification***

3. The abstract of the disclosure is objected to because it is not a single paragraph.  
Correction is required. See MPEP § 608.01(b).

#### ***Information Disclosure Statement***

4. The IDS of 3/22/2005 was considered. However, the reference to Chaum ("Zero-Knowledge undeniable signatures") does not appear to be included in the references submitted. A copy was found, considered, and is included on the Notice of references cited herewith.

#### ***Claim Objections***

5. Claims 2-7, 9 & 11-13 are objected to because of the following informalities:
  - a. Regarding claim 2, the limitation "i.e." should be replaced with "denoted as".
  - b. Regarding claim 5, the limitation "such as" should be replaced with "by".
  - c. Regarding claim 11, the limitation "calculating by the Signer the true signature" should be replaced with "calculating by the Signer a true signature".

- d. Regarding claim 12, the limitation "the check" (line 2) should be replaced with "a check".
  - e. Regarding claim 13, the limitation "the check" (line 2) should be replaced with "a check".
  - f. It is noted that any claims objected to in the heading of this section, but whose grounds for objection are not explicitly stated, are objected to based on a dependency upon an objected to claim, where appropriate.
6. Appropriate correction is required.

***Allowable Subject Matter***

7. Claims 1-13 are allowed.
8. The following is an examiner's statement of reasons for allowance, based on the above assumptions in claim clarity:
- g. Regarding claim 1, "Homomorphic Signatures Schemes" by **Johnson et al.** discloses that the RSA scheme is homomorphic (§1 & §5). Further, it is known that the RSA scheme operates on the abelian multiplicative group  $Z/mZ^*$  (see **Google Answers** reference, p. 2, second to the last posting). U.S. Patent 6,292,879 to **Gennaro et al.** discloses Undeniable Certificates, which is an undeniable signature scheme. "RSA-Based Undeniable Signatures" by **Gennaro et al.** discloses undeniable signatures, including operating on a message using a one-way function and then applying the RSA encryption scheme (see p. 138, §3). Handbook of Applied Cryptography by **Menezes et al.** teaches

the ElGamal signature scheme in the multiplicative group  $Z^*_p$  (an abelian group), applying a hash function (see p. 457, last ¶). *However, the prior art of record fails to teach or disclose, either alone or in combination, a group homomorphism (f) to obtain a resulting value (yi), in which a number of elements of an initial group (G) is larger than the number of elements (d) of a destination group (H), in combination with the other elements of the claim.*

h. Regarding claim 10, U.S. Patent 5,373,558 to **Chaum et al.** discloses confirming by a verifier a signature (Fig. 4), including obtaining a personal value from the signing (public key, see message 21 in Fig. 2), but lacks extracting a first sequence of elements from the public key, generating a second sequence of elements, randomly picking challenge parameters, computing a challenge value and verifying by the Signer, as claimed. "Convertible Undeniable Signature Scheme" by **Yun et al.** discloses an undeniable signature confirmation protocol, §3.2, but lacks the above steps. U.S. Patent 6,292,897 to **Gennaro et al.** also discloses an undeniable signature verification method (col. 4, lines 31-48), but also lacks the above steps, as claimed. "RSA-Based Undeniable Signatures" by **Gennaro et al.** discloses undeniable signatures, specifically the confirmation protocol, where elements from a public key are extracted ( $S_w$ ), random values are picked ( $i, j$ ), a challenge value is computed ( $Q$ ) (see p. 139, Fig. 1), a commitment is created ( $\text{commit}(A)$ ) and the verifier verifies that  $A$  corresponds to the value committed to by  $P$  (p. 140, ¶1), but lacks the remainder of the step discussed above, as claimed. Handbook of Applied Cryptography by **Menezes et al.** teaches the

general structure of zero-knowledge protocols, where a first party chooses a commitment (which can consist of multiple parts or iterations), a second party randomly selects a challenge, the first party sends a response and the second party checks the response to verify that the first party knows a secret without requiring the first party to reveal the secret (see p. 409, #3 and Note 10.25 (iv)). *However, the prior art of record fails to teach or disclose, either alone or in combination, the specific equations claimed as they relate to the values such as the public key, specifically, the claimed generating by the a second sequence of elements from the personal value, randomly picking the challenge parameters in sets  $G$  and  $Z_d$  as claimed, and the computing of the values  $U_i$  and  $V_i$  by the signer and verifier, respectively, in combination with the other elements of the claim.*

i. Regarding claim 11, Menezes is the closes prior art, but *differs from the claimed invention for at least the same reasons given above for claim 10. Further, the claim differs from the prior art of **Chaum, Yun and Gennaro** by claiming at least the steps of extracting by the Verifier a first sequence of elements from the public key, generating by the Verifier and Signer a second sequence of elements from the personal value, randomly picking by the Verifier challenge parameters from  $G$  and  $Z_d$  (with respect to the public key), as specifically claimed, in combination with the other elements of the claim.*

j. Claims 2-9 are allowable based on their dependence upon claim 1 and claims 12-13 are allowable based on their dependence upon claim 11.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***

9. This application is in condition for allowance except for the formal matters outlined above.

Prosecution on the merits is closed in accordance with the practice under *Ex parte Quayle*, 25 USPQ 74, 453 O.G. 213, (Comm'r Pat. 1935).

A shortened statutory period for reply to this action is set to expire **TWO MONTHS** from the mailing date of this letter.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Application/Control Number:  
10/777,661  
Art Unit: 2134

Page 7

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 3, 2007  
MJS  
/MJS/

  
KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER